**前言**

随着公司内部使用Tomcat作为web应用服务器的规模越来越大，为保证Tomcat的配置安全，防止信息泄露，恶性攻击以及配置的安全规范，特制定此Tomcat安全配置规范。

**注意：  本文章从别处转载，并做了补充**

**1. Tomcat安装规范**

注：所有线上运行tomcat必须严格安装本标准执行。

**1.1 tomcat用户设置**

[tomcat@tuan-node1 ~]# useradd -d /tomcat -u 501 tomcat

[tomcat@tuan-node1 ~]# passwd tomcat

[tomcat@tuan-node1 ~]# su - tomcat

[tomcat@tuan-node1 ~]$ id tomcat

uid=501(tomcat) gid=501(tomcat) groups=501(tomcat)

[tomcat@tuan-node1 ~]$ pwd

/tomcat

**1.2 tomcat安装**

[tomcat@tuan-node1 ~]$ wget ftp://10.6.9.111/soft/apache-tomcat-6.0.35.tgz

[tomcat@tuan-node1 ~]$ wget ftp://10.6.9.111/soft/apache-tomcat-6.0.35.tgz.md5

[tomcat@tuan-node1 ~]$ md5sum -c apache-tomcat-6.0.35.tgz.md5

apache-tomcat-6.0.35.tar.gz: OK

[tomcat@tuan-node1 ~]$ wget ftp://10.6.9.111/soft/jdk1.6.0\_22.tgz

[tomcat@tuan-node1 ~]$ wget ftp://10.6.9.111/soft/jdk1.6.0\_22.tgz.md5

[tomcat@tuan-node1 ~]$ md5sum -c jdk1.6.0\_22.tgz.md5

jdk1.6.0\_22.tgz: OK

[tomcat@tuan-node1 ~]$ tar xzf apache-tomcat-6.0.35.tgz

[tomcat@tuan-node1 ~]$ tar xzf jdk1.6.0\_22.tgz

**1.3 tomcat配置**

[tomcat@tuan-node1 ~]$ vim .bash\_profile 增加以下内容：

export JAVA\_HOME=/tomcat/jdk1.6.0\_22

export PATH=$JAVA\_HOME/bin:$JAVA\_HOME/jre/bin:$PATH

export CLASSPATH=.$CLASSPATH:$JAVA\_HOME/lib:$JAVA\_HOME/jre/lib:$JAVA\_HOME/lib/tools.jar

export TOMCAT\_HOME=/tomcat/apache-tomcat-6.0.35

[tomcat@tuan-node1 ~]$source .bash\_profile

[tomcat@tuan-node1 ~]$ java -version

java version "1.6.0\_26"

Java(TM) SE RuntimeEnvironment(build 1.6.0\_26-b03)

JavaHotSpot(TM)64-BitServer VM (build 20.1-b02, mixed mode)

**1.4 应用程序配置**

[tomcat@tuan-node1 ~]$ mkdir webapps

将应用程序放置在/tomcat/目录下。建立相应的目录如团购wmw\_tuan，静态化wmw\_static，并修改server.xml，对应好目录即可。

**1.5 启动Tomcat：**

[tomcat@tuan-node1 ~]$ /tomcat/apache-tomcat-6.0.35/bin/startup.sh

Using CATALINA\_BASE:   /tomcat/apache-tomcat-6.0.35

Using CATALINA\_HOME:   /tomcat/apache-tomcat-6.0.35

Using CATALINA\_TMPDIR:/tomcat/apache-tomcat-6.0.35/temp

Using JRE\_HOME:        /tomcat/jdk1.6.0\_22

Using CLASSPATH:       /tomcat/apache-tomcat-6.0.35/bin/bootstrap.jar

**2 . 安全设置规范**

**2.1 telnet管理端口保护（强制）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置** | **备注** |
| telnet管理端口保护 | 1.修改默认的8005管理端口为不易猜测的端口（大于1024）；  2.修改SHUTDOWN指令为其他字符串； | <Server port="**8527**" shutdown="**dangerous**"> | 1.以上配置项的配置内容只是建议配置，可以按照服务实际情况进行合理配置，但要求端口配置在**8000~8999**之间； |

**2.2 ajp连接端口保护（推荐）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置** | **备注** |
| Ajp 连接端口保护 | 1.修改默认的ajp 8009端口为不易冲突的大于1024端口；  2.通过iptables规则限制ajp端口访问的权限仅为线上机器； | <Connector port="**8528**"  protocol="AJP/1.3" /> | 以上配置项的配置内容仅为建议配置，请按照服务实际情况进行合理配置，但要求端口配置在**8000~8999**之间；；  保护此端口的目的在于防止线下的测试流量被mod\_jk转发至线上tomcat服务器； |

**2.3 禁用管理端（强制）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置** | **备注** |
| 禁用管理端 | 1. 删除默认的{Tomcat安装目录}/conf/tomcat-users.xml文件，重启tomcat后将会自动生成新的文件；  2. 删除{Tomcat安装目录}/webapps下默认的所有目录和文件；  3.将tomcat 应用根目录配置为tomcat安装目录以外的目录； | <Context path="" docBase="**/home/work/local/tomcat\_webapps**" debug="0" reloadable="false" crossContext="true"/> | 对于前段web模块，Tomcat管理端属于tomcat的高危安全隐患，一旦被攻破，黑客通过上传web shell的方式将会直接取得服务器的控制权，后果极其严重； |

**2.4 降权启动（强制）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置** | **备注** |
| 降权启动 | 1.tomcat启动用户权限必须为非root权限，尽量降低tomcat启动用户的目录访问权限；  2.如需直接对外使用80端口，可通过普通账号启动后，配置iptables规则进行转发； | - | 避免一旦tomcat 服务被入侵，黑客直接获取高级用户权限危害整个server的安全； |

**2.5 文件列表访问控制（强制）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置** | **备注** |
| 文件列表访问控制 | 1.conf/web.xml文件中default部分listings的配置必须为false； | <init-param>  <param-name>**listings**</param-name>  <param-value>**false**</param-value>  </init-param> | false为不列出目录文件，true为允许列出，默认为false； |

**2.6 版本信息隐藏（强制）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置** | **备注** |
| 版本信息隐藏 | 1.修改conf/web.xml，重定向403、404以及500等错误到指定的错误页面；  2.也可以通过修改应用程序目录下的WEB-INF/web.xml下的配置进行错误页面的重定向； | <error-page>  <error-code>**403**</error-code>  <location>**/forbidden.jsp**</location>  </error-page>  <error-page>  <error-code>**404**</error-code>  <location>**/notfound.jsp**</location>  </error-page>  <error-page>  <error-code>**500**</error-code>  <location>**/systembusy.jsp**</location>  </error-page> | 在配置中对一些常见错误进行重定向，避免当出现错误时tomcat默认显示的错误页面暴露服务器和版本信息；  必须确保程序根目录下的错误页面已经存在； |

**注意： 此外的错误页面定义，每个项目工程目录下都要各自建立自己的相应的错误页面。**

**2.7 Server header重写（推荐）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置** | **备注** |
| Server header重写 | 在HTTP Connector配置中加入server的配置； | server="**webserver**" | 当tomcat HTTP端口直接提供web服务时此配置生效，加入此配置，将会替换http 响应Server header部分的默认配置，默认是Apache-Coyote/1.1 |

**2.8 访问限制（可选）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置或操作** | **备注** |
| 访问限制 | 通过配置，限定访问的ip来源 | <Context path="" docBase="/home/work/tomcat" debug="0" reloadable="false" crossContext="true">  <Valve className="org.apache.catalina.valves.RemoteAddrValve"**allow="61.148.18.138,61.135.165.\*" deny="\*.\*.\*.\*"**/>  </Context> | 通过配置信任ip的白名单，拒绝非白名单ip的访问，此配置主要是针对高保密级别的系统，一般产品线不需要； |

**注意：Tomcat6和Tomcat8此处的区别，下面是tomcat8的写法**

<Valve className="org.apache.catalina.valves.RemoteAddrValve"  
allow="192\.168\.234\.\d+|127\.\d+\.\d+\.\d+|::1|0:0:0:0:0:0:0:1"/>  
允许本地回环地址及192.168.234.0网段访问

**2.9 起停脚本权限回收（推荐）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置或操作** | **备注** |
| 起停脚本权限回收 | 去除其他用户对Tomcat的bin目录下shutdown.sh、startup.sh、catalina.sh的可执行权限； | chmod -R 744 tomcat/bin/\* | 防止其他用户有起停线上Tomcat的权限； |

**2.10 访问日志格式规范（推荐）**

|  |  |  |  |
| --- | --- | --- | --- |
| **类别** | **配置内容及说明** | **标准配置或操作** | **备注** |
| 访问日志格式规范 | 开启Tomcat默认访问日志中的Referer和User-Agent记录 | <Valve className="org.apache.catalina.valves.AccessLogValve"  directory="logs"  prefix="localhost\_access\_log." suffix=".txt"  pattern="%{X-Forwarded-For}i %l %u %t %r %s %b %{Referer}i %{User-Agent}i %D" resolveHosts="false"/> | 开启Referer和User-Agent是为了一旦出现安全问题能够更好的根据日志进行问题排查；  X-Forwarded-For用于nginx作为反向代理服务器时，获取客户端真实的IP |

**2.11 屏蔽DNS查询**

enableLookups：调用request、getRemoteHost()执行DNS查询，以返回远程主机的主机名，如果设置为false，则直接返回IP地址。

<Connector enableLookups="false"/>

**2.12  压缩管理**

tomcat作为一个应用服务器，也是支持 gzip 压缩功能的。我们可以在 server.xml 配置文件中的 Connector 节点中配置如下参数，来实现对指定资源类型进行压缩。 前端使用nginx作为反向代理，一般不需要启用tomcat压缩功能。

**compression="on" # 打开压缩功能**

**compressionMinSize="50" # 启用压缩的输出内容大小，默认为2KB**

**noCompressionUserAgents="gozilla, traviata" # 对于以下的浏览器，不启用压缩**

**compressableMimeType="text/html,text/xml,text/javascript,text/css,text/plain"# 哪些资源类型需要压缩**

**3. 附录：建议配置及标准执行方案**

**3.1 配置部分（${ CATALINA\_HOME }conf/server.xml）**

<Server port="8527" shutdown=" dangerous">

<!--Define a non-SSL HTTP/1.1Connector on port 8080-->  
<Connector port="8080" server="webserver"/>

<!--Define an AJP 1.3Connector on port 8528-->  
<!--Define an accesslog -->  
<Valve className="org.apache.catalina.valves.AccessLogValve" directory="logs"  prefix="localhost\_access\_log." suffix=".txt"  
pattern="%h %l %u %t %r %s %b %{Referer}i %{User-Agent}i %D" resolveHosts="false"/>

<Connector port="8528" protocol="AJP/1.3"/>

<Context path="" docBase="/home/work/local/tomcat\_webapps" debug="0" reloadable="false" crossContext="true"/>

**3.2 配置部分（${ CATALINA\_HOME }conf/web.xml或者WEB-INF/web.xml）**

<init-param>  
       <param-name>listings</param-name>  
       <param-value>false</param-value>  
</init-param>

<error-page>  
       <error-code>403</error-code>  
       <location>/forbidden.jsp</location>  
</error-page>  
<error-page>  
       <error-code>404</error-code>  
       <location>/notfound.jsp</location>  
</error-page>  
<error-page>  
       <error-code>500</error-code>  
       <location>/systembusy.jsp</location>  
</error-page>

**3.3 删除如下tomcat的默认目录和默认文件**

tomcat/webapps/\*

tomcat/conf/tomcat-user.xml

**3.4 去除其他用户对tomcat 起停脚本的执行权限**

chmod 744 –R tomcat/bin/\*